

**FILED - GR**

August 8, 2023 11:00 AM

CLERK OF COURT

U.S. DISTRICT COURT

WESTERN DISTRICT OF MICHIGAN

BY:JMW SCANNED BY: JA / 82

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION**

DAVID ANGEL SIFUENTES III,  
Plaintiff,

CASE NO.  
HONORABLE:

**1:23-cv-834**  
**Paul L. Maloney**  
**United States District Judge**

V.

AT&T,

Defendant.

DEMAND FOR JURY TRIAL

**COMPLAINT WITH MEMORANDUM OF LAW AND DEMAND FOR  
JURY TRIAL**

Now comes, the Plaintiff David Angel Sifuentes III, In Pro Se and submits complaint with memorandum of law and demand for jury trial, Sifuentes asserts that his property that is data was deprived of the security interest and adequate process to protection and seeking relief for identity theft, personal information, (data) being exposed and stolen from a data breach from At&t., which Sifuentes has Diversity Standing for "imminent" risk of identity theft or fraud" to bring this complaint. *See In re Zappos.com, Inc.*, 884 F.3d 893 (9<sup>th</sup> Cir. 2018), *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App'x 384 (6<sup>th</sup> Cir. 2016), violation of Texas deceptive Trade Practices, Texas Unfair methods of competition and unfair or deceptive acts or practice prohibited act, invasion of privacy by public disclosure of private facts, negligence, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, negligent and or intentional infliction of emotional distress, conversion (use of information without permission) breach of bailment, failure to promptly notify of the breach and provide security measures and protection to Sifuentes for the breach, and risk of future injury, Identity Theft Protection Act MCL 445.72, also the Michigan Consumers Protection Act. Sifuentes is seeking damages of \$375,000.00 and punitive damages of \$300,000,000.00 for a total of \$300,375,000.

Sifuentes ask this Court to liberally construe his pleadings, legal documents, arguments and not fault him for not citing are applying the correct case law, statute and applicable laws under *Haines v. Kerner*, 404 U.S. 519 (1972). Pro se litigants can be excused from full compliance with technical procedural rule, provided there is substantial compliance. *Norefleet v. Walker*, 684 F.3d

688 (7<sup>th</sup> Cir. 2012). Court and staff have a special responsibility to scrutinize carefully pro se complaints. *Chapman v. Kleindienst*, 507 F.2d 1246, 1253 (7<sup>th</sup> Cir. 1974) (district court has responsibility for finding hidden jury demands in the middle of complaints). ). A court must accept all allegations of well-plead factual allegations as true, *League Am. Citizens v. Bredesen*, 500 F.3d 523, 527 (6<sup>th</sup> Cir. 2007), and factual allegations alone is what matters. *Albert v. Carovano*, 851 F.2d 561, 571 n.3 (2<sup>nd</sup> Cir. 1988). Please note that Sifuentes relies on his exhibits he filed on November 28, 2022 with his original complaint in support of this amended complaint.

### **Jurisdiction**

This court has **diversity jurisdiction** of all state law claims under this complaint, as At&t is a citizen of Texas and is a cooperation head quartered in Dallas, Texas David Angel Sifuentes III is a citizen of Grand Rapids, Michigan, and therefore the parties are different citizens from different states and this court has jurisdiction of all civil matters as the damages are more than \$75,000 28 U.S.C. § 1332, therefore they are citizens of different states and diversity jurisdiction exists for this court to allow his state law claims to proceed in this Court. *See Wis. Dep't of Corr. v. Schacht*, 524 U.S. 381, 388 (1998), also since Texas is the principal place of business for AT&T where they are headquartered. *Hertz Corp. v. Friend*, 559 U.S. 77 (2010). Sifuentes is seeking damages of \$375,000.00 and punitive damages of \$350,000,000.00, which can also be added for jurisdictional purposes. *Hayes v. Equitable Energy Res. Co.*, 226 F3d 560 (6<sup>th</sup> Cir. 2001).

This court also has personal jurisdiction under the “minimum contacts” rule as Sifuentes received services from At&t being phone service and an account via online in Michigan. Pursuant to MCL 600.711, a Michigan court may exercise general personal jurisdiction over a defendant-corporation if: (1) it is incorporated under the laws of Michigan; (2) the defendant has consented to personal jurisdiction in Michigan; or (3) the corporation “carr[ies] on... a continuous and systematic part of its general business within the state.”

Michigan’s long-arm statute “has been construed as conferring on the state courts the maximum scope of personal jurisdiction consistent with due process.” *Amway Corporation v. Kope Food Products, Inc.*, 840 F. Supp. 78, 80 (W.D. Mich. 1993). The exercise of limited

jurisdiction “occurs where ‘a State exercises jurisdiction over a defendant in a suit arising out of or related to the defendant’s contacts with the forum.’” *Kmart Corp. v. Key Industries, Inc.*, 877 F. Supp. 1048, 1051 (E.D. Mich. 1994), quoting *Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414 n. 9 (1984). Michigan extends limited jurisdiction over nonresident corporations pursuant to MCL § 600.715. Pursuant to Michigan’s Long Arm Statute, MCL 600.715, “a sufficient basis of jurisdiction to enable a court of record of this state to exercise limited personal jurisdiction” exists when a corporation’s acts “create any of the following relationships: (1)[t]he transaction of any business within the state” or “(2) [t]he doing or causing an act to be done, or consequences to occur, in the state resulting in an action for tort.” In interpreting MCL 600.715, the Michigan Supreme Court has held that “[t]he word ‘any’ means just what it says. It includes ‘each’ and ‘every.’ It comprehends ‘the slightest.’” *Sifers v Horen* 385 Mich 195, 199 n 2, 188 NW2d 623 (1971).

Federal courts have a “virtually unflagging obligation to exercise jurisdiction which is given, than to usurp that which is not given,” *Cohens v. Virginia*, 19 U.S. (6 Wheat.) 264, 404 (1821). Thus, when diversity jurisdiction is properly invoked, federal courts have a “duty... to decide questions of state law whenever necessary to the rendition of a judgment.” *Meredith v. City of Winter Haven*, 320 U.S. 228, 234 (1943); see *Burgess v. Seligman*, 107 U.S. 20, 33 (1883) (explaining that “[t]he federal courts have an independent jurisdiction in the administration of state laws, co-ordinate with, and not subordinate to, that of state courts”). It is still the duty of the federal courts, where the state law supplies the rule of decision, to ascertain and apply that law even though it has not been expounded by the highest court of the State.” *Fid. Union Tr. Co. v. Field*, 311 U.S. 169, 177 (1940).

**“Standard of Review” Article III standing “personal injury”**

Article III. Section 2 of the United States Constitution:

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;--to all Cases affecting Ambassadors, other public Ministers and Consuls;--to all Cases of admiralty and maritime Jurisdiction;--to Controversies to which the United States shall be a Party;--to Controversies between two or more States;-- between a State and Citizens of another State;-- between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

Article III confines the federal judicial power to the resolution of “Cases” and “Controversies” in which a plaintiff has a ‘personal stake. “To have Article III standing to sue in federal court, a plaintiff must show, among other things, that the plaintiff suffered concrete injury in fact. Central to assessing concreteness is whether the asserted harm has “close relationship” to harm “traditionally” recognized as providing a basis for a lawsuit in American courts. That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury. Physical or monetary harms readily qualify s concrete injuries under Article III, and various intangible harms-like reputational harms-can also be concrete. *Transunion LLC v. Ramirez*, 141 S.Ct. 2190, 2198 (2021).

Plaintiff’s have Article III standing and Sifuentes has standing of the United States Constitution in this court to his data breach complaint. *See In re Zappos.com, Inc.*, 884 F.3d 893 (9<sup>th</sup> Cir. 2018), *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App’x 384 (6<sup>th</sup> Cir. 2016). The United States Supreme Court has “found standing based on a ‘substantial risk’ that the harm will occur even if not literally certain the harms will come about. *Galaria, supra citing (Clapper v. Amnsesty Int’l USA*, 133 S.Ct. 1138, 1150 n.5).

Sifuentes asserts that he has Article III standing for his data breach claim personal injury theft of his identity. The Sixth Circuit has found that Plaintiff’s allegations were sufficient to establish Article III standing at the pleading stage of the litigation though allegations of actual fraud and identity theft were absent: “Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of ‘possible future injury ‘or “objectively reasonable likelihood’ of injury that the Supreme Court has explained are insufficient.” *Id.* at \*9 (*quoting Clapper*, 133 S.C.t at 1147-48).

### **Timing**

Sifuentes claims are timely under Michigan, law MCL 600.5805., as Sifuentes was notified on March 22, 2023.

**Facts**

On or around March 22, 2023 Sifuentes obtained an email from At&t, Exhibit A, Email from At&T, March 22, 2023, informing him that his private data had been stolen. Although At&t claim that the information did not contain sensitive information any data that someone would steal that is important and may easily lead to access of doors to gain more valuable information also discovery may reveal otherwise. At&t failed to secure and protect through careless security and negligence personal information concerning Sifuentes personal information such as the Customer Proprietary Network Information (CPNI). Further facts may be presented in this pleading.

**Judicial Notice**

Pursuant to Fed. R. Evid. 201(c)(2), the Court “must take judicial notice if a party requests it and the court is supplied with the necessary information.” Types of facts that may be judicially noticed include those that “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” Fed.R.Evid. 201(b)(2). This includes materials that are in the public record. *New England Health Care Employees Pension Fund v. Ernst & Young, LLP*, 336 F.3d 495, 501 (6<sup>th</sup> Cir. 2003)(“A court that is ruling on Rule 12(b) motion may consider materials in addition to the complaint if such materials are public records or are otherwise appropriate for the taking of judicial notice.”); *Rodic v. Thistledown Racing Club, Inc.*, 615 F.3d 736, 738 (6<sup>th</sup> Cir. 1980) (“Federal courts may take judicial notice of proceedings in other courts of record.”). Sifuentes ask that this Court take judicial notice of Exhibits A At&t’s email, and also the following articles discussed on the effects and worth of data.

**The effects and worth of data.**

Sifuentes ask that this Honorable Court take judicial notice of the following public online articles in support of his complaint. Data personal identifier information (PII) is very valuable and priceless as there is unlimited potential for cybercriminal’s to do harm. PII is valuable property. See Articles online Marc Van Lieshout, *The Value of Personal Data at p. 4, 457 IFIP*

*ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY* 26 (MAY 10, 2015), available at [https://researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data\\_9](https://researchgate.net/publication/283668023_The_Value_of_Personal_Data_9)”The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]” (last visited April 11, 2023).

Companies such as At&T profit from data used from At&T Firms are able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing regulatory and legal frameworks. See *Exploring the Economics of Personal Data: A Survey of methodologies for Measuring Monetary Value*, OECD Digital Economic Papers no. 220 (Apr. 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en) (last visited April 11, 2023). See *U.S. Firms to Spend Nearly \$19.2 billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/> (last visited April 11, 2023).

PII can be sold from anywhere from \$40 to \$200, and bank details have a price range of \$50 to \$200. Anita George, *Your personal data is for sale on the dark web*. Here’s how much it costs, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited April 11, 2023). Criminals can also purchase entire data breaches from \$900 to \$4,500. In the Dark, VPNOverview.com, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed on April 4, 2023). Experian has found that stolen debit and credit cards details can sell for \$5 to \$110 on the dark web. Brian Stack, *Here’s How Much Your Personal Information is Selling for on the Dark Web*, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited April 11, 2023).

At&T collects and sells information concerning phone plans and other personal information concerning consumers and their habits, as consumers place a high value on the privacy of that data. There has been research that sheds light on how much consumers value their data privacy and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites. Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) *INFORMATION SYSTEMS RESEARCH* 254 (June 2011), <https://www.jstor.org/stable/23015560?seq=1> (last visited April 4, 2023).

Cyberattacks have become so frequent that the U.S. Secret Service and FBI have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals...because they often have a lesser IT defenses and a high incentive to regain access to their data quickly. Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited April 4, 2023).

Data is very valuable and criminals have a need to use that property that is individuals PII.

### **Complaint and memorandum**

#### **i. Violation of Texas deceptive Trade Practices Unlawful, Texas Unfair methods of competition and or deceptive acts or practices prohibited Article III “concrete injury” “imminent” risk of identity theft or fraud”.**

At&t has violated the Texas deceptive Trade Practices Chapter 17. Sec.17.46 et. seq. and Texas unfair methods of competition and unfair deceptive acts or practices, Chapter 541 Sec 541.003 et. seq. for not providing adequate protection and property interest of Sifuentes personal data information stored with At&t.

Here that interest was not protected by At&t and they deprived Sifuentes of the security measures and procedural protections also adequate process to protect the (CPNI). Sifuentes personal information his identity that is facts that represent his reputation have been taken and could be used to commit future crimes and create imminent danger and risk. On or about March 22, 2023 Sifuentes found that he was a victim of a data breach from At&t f (See Exhibit “A”) notifying him that his data PII personal information had been compromised. A data breach victim may seek relief in Federal Court when a company has failed to protect the data of its customers. See *Galaria v. Nationwide Mutual Insurance Co.*, 663 F.App’x 384 (6<sup>th</sup> Cir. 2016). This includes heightened risk of future injury, *In re U.S. Office of Personnel Management Data*, 928 F.3d 42 (D.C. Cir. 2019). A litigant need not provide proof of monetary damage to bring a claim of data breach in Federal Court. A plaintiff threatened with future injury has standing to sue “if the threatened injury is ‘certainly impending,’ or the risk that the harm will occur. See *In*

*re Zappos.com, Inc.*, 884 F.3d 893 (9<sup>th</sup> Cir. 2018). A litigant need only provide *concrete proof* that his personal information had been comprised by the breach. See *Transunion LLC v. Ramirez*, 141 S.Ct. 2190 (2021).

Sifuentes has shown in injury in fact and concrete injury of the data breach where his identity has been stolen that is his personal data and information from At&t which includes his name, and (CPNI), such information can and has been comprised which leads to hackers using the data to commit crime are assume the Identity of Sifuentes that is identity theft a concrete injury, *Transunion LLC, v. Ramirez*, 141 S.Ct. 2190 (2021); *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App'x 384 (6<sup>th</sup> Cir. 2016); *Clemens v. ExecuPharm Inc.*, 48 F.4<sup>th</sup> 146 (3<sup>rd</sup> Cir. 2022):

Article III standing requires a plaintiff to demonstrate.” (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief. this court does not have jurisdiction and his state law claims should proceed in federal court.Id., citing cases.

Here the data breach occurred that is theft of Sifuentes identity, two the injury-in-fact is actual or imminent as the data from At&t that is (CPNI) personal facts still and endure the kind of future harm that qualifies as ‘imminent.’ *Clemens v. ExecuPharm Inc.*, 48 F.4<sup>th</sup> 146, 152 (3<sup>rd</sup> Cir. 2022). The data could be used to open bank accounts and other accounts and commit crime that is cybercrimes with it.

**ii. Invasion of privacy by public disclosure of private facts, intentionally, willfully, recklessly, and negligently failed to protect data.**

Sifuentes has suffered invasion of privacy by public disclosure of private facts where his personal information PII data has been exposed and stolen and taken without him knowing and without permission his peroneal property being his data from At&t. At&t ‘intentionally, willfully, recklessly, and negligently” failed to take sufficient measures to safeguard the data. At&t did not follow the guidelines for a data breach as required by the Federal Trade Commission. Sifuentes has indeed suffered concrete injury in fact, due to the exposure of his personal information. *TransUnion v. Ramirez*, 141 S.Ct. 2190 (2021).

**iii. Bailment**

At&t has violated bailment, failure to promptly notify of the breach and provide security measures and protection to Sifuentes for the breach. Here Sifuentes delivered valuable digital information that is his property and trusted that information would be secured to At&t. The goods or At&t collection of data and information., (CPNI). Without the information At&t would not be in business because they use data to make profit, See Article *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018)*, <https://www.iab.com/news/2018-state-of-data-report/> (last visited March 18, 2023).

As Blacks law dictionary 6<sup>th</sup> edition defines Bailment as:

A delivery of goods or personal property, by one person (bailor) to another (bailee), in trust for the execution of a special object upon or in relation to such goods, beneficial either to the bailor or bailee or both, and upon a contract, express or implied, to perform the trust and carry out such object, and thereupon either to redeliver the goods to the bailor or otherwise dispose of the same in conformity with the purpose of the trust.  
The bailee is responsible for exercising due care toward the goods....  
p. 141-142.

Definitely data is goods and valuable and worth a lot of money to data thieves See Article *Brian Stack, Here's How Much Your Personal Information Is Selling for in the Dark Web, Experian (Dec. 6, 2017)*, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited March 18, 2023).

**iv. Negligence**

At&t owed a duty to Sifuentes to protect his data on At&t to exercise reasonable care in safeguarding and protecting his PII in tis possession, custody, or control. At&t knew, or should of known, the risks of collecting and storing Sifuentes and other users personal tweets and data, and the importance of maintaining secure systems. At&t knew, or should have known, of the vast uptick in data breaches in recent years. At&t had a duty to protect the PII of Sifuentes.

Given the nature of At&t's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, At&t should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which At&t had a duty to prevent.

At&t breached these duties by failing to exercise reasonable care in safeguarding and protecting Sifuentes's PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to-including Sifuentes PII.

**v. Negligence Per Se**

At&t duties rise from Texas deceptive trade practices and unfair methods of competition and or deceptive acts or practices prohibited act and Michigan Consumer protection act prohibiting deceptive practices, which prohibits "unfair... practices in or affecting commerce," including, as interpreted by Texas and Michigan, the unfair act or practice by a business, such as At&t, of failing to employ reasonable measures to protect and secure PII.

At&t violated Texas deceptive trade practices and unfair methods of competition and or deceptive acts or practices prohibited act and Michigan Consumer protection act prohibiting deceptive practices by failing to use reasonable measures to protect Sifuentes and all other users affected by the breach, and not complying with applicable industry standards. At&t's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of data breach involving PII including, specifically, the substantial damages that would result to Sifuentes. At&t's violations of these acts constitutes negligence per se.

**vi. Breach of fiduciary duty**

Sifuentes and users either directly or indirectly gave At&t their PII in confidence, believing that At&t would protect that information. Sifuentes and users would not have provided At&t with this information had they known it would not be adequately protected. At&t's acceptance and storage of Sifuentes's created a fiduciary relationship between At&t and Sifuentes. In light of this relationship, At&t must act primarily for the benefit of its customers, which includes safeguarding and protecting Sifuentes's PII.

At&t has a fiduciary duty to act for the benefit of Sifuentes and upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Sifuentes's and users PII, failing to comply with the data security guidelines set forth by Texas deceptive trade practices and unfair methods of competition and or deceptive acts or practices prohibited act and Michigan Consumer protection act prohibiting deceptive practices, and otherwise failing to safeguard the PII it collected and collects.

**vii. Unjust Enrichment**

Data is a business and At&t collects a monetary benefit upon users, and selling data. At&t accepted or had knowledge of the benefits conferred upon it by Sifuentes. At&t also benefited from the receipt of Sifuentes and At&t users. Sifuentes paid for phone service and provided financial information for his phone account.

As a result of At&t's conduct, Sifuentes suffered actual damages in an amount equal to the difference in value between his valuable data used to make profit made with reasonable data privacy and security practices and procedures that Sifuentes and other customer's paying At&t users without reasonable data privacy and security practices and procedures that they received.

**viii. Breach of Implied Contract**

At&t required Sifuentes and users to provide, or authorize the transfer of, their PII in order for At&t to provide services. Also phone agreement In exchange, At&t entered into implied contracts with Sifuentes in which At&t agreed to comply with its statutory and common law duties to protect Sifuentes's PII and to timely notify him in the event of a data breach.

Sifuentes would not have provided his PII to At&t had he known that At&t would not safeguard his PII, as promised, or provide timely notice of a data breach.

**ix. Negligent and or intentionally infliction of emotional distress.**

Sifuentes is going through negligent and intentional infliction of emotional distress as his personal information has been stolen for nearly two years plenty of time for hackers and cyber

criminals to cause harm. It is “fairly traceable” that the stolen data for At&t may indeed cause Sifuentes other accounts to be hacked by cyber criminals. This is stressful and Sifuentes is scared as hackers can commit crimes with his personal information.

**x. Risk of future and ongoing injury.**

Sifuentes has presented actions which might suffer future concrete injury. *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016). Here the data breach occurred that is theft of Sifuentes identity, two the injury-in-fact is actual or imminent as the data from At&t that is (CPNI), personal facts still and endure the kind of future harm that qualifies as ‘imminent.’ *Clemens v. ExecuPharm Inc.*, 48 F.4<sup>th</sup> 146, 152 (3<sup>rd</sup> Cir. 2022). The data could be used to open bank accounts and other accounts and commit crime that is cybercrimes with it. Sifuentes case does raise and Article III standing where his identity has been stolen that is his personal data and information from At&t (CPNI) which includes his name and other personal information, such information can and has been comprised which leads to hackers using the data to commit crime are assume the Identity of Sifuentes that is identity theft a concrete injury, *Transunion LLC, v. Ramirez*, 141 S.Ct. 2190 (2021); *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App’x 384 (6<sup>th</sup> Cir. 2016); *Clemens v. ExecuPharm Inc.*, 48 F.4<sup>th</sup> 146 (3<sup>rd</sup> Cir. 2022).

**xi. Conversion**

At&t is in violation of conversion that is unauthorized assumption and exercise of the right of ownership over goods or personal data belonging to Sifuentes. The data breach was an unauthorized act depriving Sifuentes of his personal property that is his PII with At&t.

This was inconsistent violation of conversion wrongful exercise of Sifuentes personal property that is his PII.

**xii. Michigan Consumer protection Act.**

At&t is in violation of the Michigan Consumer Protection Act Mich. Comp. Laws Ann § 445.901 for deceptive practices by covering up the breach and not notifying him of the breach. Also misrepresenting that the goods being data was protected.

At&t failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach.

**xii. Identity Theft Protection Act MCL 445.72.**

For the reasons discussed in this complaint At&t is in violation of the Identity Theft Protection Act MCL 445.72 law. As mentioned earlier they did not provide adequate security measures and protect Sifuentes PII.

**xiv. Damages**

As discussed data is valuable , priceless, and Sifuentes requests for damages is reasonable in this matter as there is unlimited potential for criminals to recycle and continue to use Sifuentes personal data also many other users. Sifuentes is seeking \$375,000.00 for actual damages for injuries caused by both negligent and intentional infliction of emotional distress such as being very mad, angry, and sacred, worried, nervous and has trouble sleeping and scared of what else hackers whole stole his information will do as they keep accessing his accounts and his information is in the dark web., also bank account opened under his name.

Sifuentes seeks \$300,000,000.00 in exemplary, economic and non-economic damages, compensatory and punitive damages injunctive and declaratory relief as this is calculated from the fines and penalties associated from companies concealing data breaches from victims such as the Equifax which settled for \$575,000,000 Capital data breach that settled for \$190 million for failing to take action with data breach protocols.

**RELIEF REQUESTED**

**WHEREFORE,** Sifuentes **PRAYS** that this Honorable court grant relief as follows:

Award Sifuentes \$375,000.00 in actual damages for negligent and intentional infliction of ongoing emotional distress for being mad upset and under stress and \$300,000,000.00 in exemplary, compensatory and punitive damages injunctive and declaratory relief, for a total of \$300,375,000 or in the alternative Award \$300,000.00 in actual damages and that At&t provide Sifuentes with 5 years of LifeLock to help clean and restore Sifuentes identity.

Respectfully submitted,

By: 

Plaintiff In Pro Se

David Angel Sifuentes III

439 More St. NE

Grand Rapids, MI 49503

(616)283-5215

[davidsifuentes61@yahoo.com](mailto:davidsifuentes61@yahoo.com)

DATED: August 5, 2023

David Angel Sifuentes III  
439 More St. NE  
Unit 2  
Grand Rapids, MI 49503

Clerk  
399 Federal  
110 Michigan  
Grand Rapids

**Retail**



49503

**RDC 99**

U.S. POSTAGE PAID  
FCM LG ENV  
GRAND RAPIDS, MI 49501  
AUG 05, 2023

**\$2.31**

R2304M109975-08

Bldg  
n St. NW  
s, MI 49503